AMENDMENTS TO THE CLAIMS

Claims 1-36 are pending. Please amend claims 1-31 and 33-36. Kindly cancel claim 32 without prejudice. No claims are added.

The following listing of claims replaces all prior versions, and listings of claims in the application.

1. (Currently amended) A computer-implemented method for a computer-program module to provide application security threat-modeling, the method comprising:

providing class definitions for ~~defining~~ a plurality of model components to represent respective elements of an application, each model component specifying a set of security threat categories potentially applicable to the component ~~comprising a respective set of potential security threats~~;

responsive to user input, interconnecting at least a subset of the model components to form a logical model of the application; and

automatically analyzing the at least a subset of model components and respective interconnections to identify a set of potential security threats corresponding to the at least a subset, the potential security threats being associated with one or more of the security threat categories~~one or more of the potential security threats in terms of the model components in the logical model~~.

2. (Currently amended) ~~A~~ The method ~~as recited in~~ of claim 1, wherein the model components comprise a module, a port, a store, or a wire.

3. (Currently amended) ~~A~~ The method ~~as recited in~~ of claim 1, wherein the security threat categories ~~potential security threats~~ comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation.

4. (Currently amended) ~~A~~ The method ~~as recited in~~ of claim 1, wherein ~~defining the model components~~ providing the class definitions further comprises determining the ~~respective~~ security threat ~~characteristics~~ categories ~~for a component of the model components~~ based on ~~the components corresponding~~ functionality of the component with respect to ~~in~~ the application.

5. (Currently amended) ~~A~~ The method ~~as recited in~~ of claim 1, wherein analyzing ~~one or more of the potential threats in terms of the model components~~ further comprises~~:~~ responsive to ~~selecting~~ selection of a ~~the~~ particular component of the model components, displaying each other component of the at least a subset ~~model components~~ that comprise at least a subset of similar potential security threats categories as the particular component.

6. (Currently amended) ~~A~~ The method ~~as recited in~~ of claim 1, wherein analyzing ~~one or more of the potential threats in terms of the model components~~ further comprises~~:~~ ~~selecting a particular component of the model components; and~~responsive to ~~selecting the~~ selection of a particular component of the at least a subset, automatically displaying each other component of the ~~model components~~ at least a subset that comprises a particular security threats similar to a security threat already addressed with respect to the particular component.

7. (Currently amended) ~~A~~ The method ~~as recited in~~ of claim 1, wherein analyzing ~~one or more of the potential security threats in terms of the model components in the logical model~~ further comprises: ~~selecting~~ providing for selection of a particular threat associated with the security threat categories ~~of the potential threats~~ to indicate that the particular threat requires a threat mitigating implementation in a particular ~~mode~~ model component of the at least a subset ~~model components, the particular threat corresponding to the particular model component~~.

8. (Currently amended) ~~A~~ The method ~~as recited in~~ of claim 7 ~~5~~, wherein ~~selecting~~ providing for selection of the particular threat further comprises identifying a priority ~~that corresponds to~~ of the threat mitigating implementation.

9. (Currently amended) ~~A~~ The method ~~as recited in~~ of claim 7, wherein ~~selecting~~ providing for selection of the particular threat further comprises identifying a desired level of strength of technology with which to mitigate the particular threat.

10. (Currently amended) ~~A~~ The method ~~as recited in~~ of claim 7, wherein ~~selecting~~ providing for selection of the particular threat further comprises ~~selecting~~ presenting information associated with a particular technology with which to mitigate the one or more potential threats in a physical implementation of the application.

11. (Currently amended) A computer-readable medium comprising computer-executable instructions for providing application security threat-modeling, the computer-executable instructions comprising instructions for:

defining a plurality of model components to represent respective elements of an application, each model component specifying a set of security threat categories potentially applicable to the component ~~comprising a respective set of potential security threats~~, the model components being defined with class definitions in a component schema;

interconnecting, responsive to user input, at least a subset of the model components to form a logical model of the application; and

analyzing the at least a subset and respective interconnections to identify a set of potential security threats associated with associated ones of the security threat categories~~one or more of the potential security threats in terms of the model components in the logical model~~.

12. (Currently amended) ~~A~~ The computer-readable medium ~~as recited in~~ of claim 11, wherein the model components comprise a module, a port, a store, or a wire.

13. (Currently amended) ~~A~~ The computer-readable medium ~~as recited in~~ of claim 11, wherein the security threat categories ~~potential security threats~~ comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation.

14. (Currently amended) ~~A~~ The computer-readable medium ~~as recited in~~ of claim 11, wherein the computer-executable instructions for defining the model components further comprise instructions for determining the ~~respective~~ security threat ~~characteristics~~ categories for a component of the model components based on ~~the components corresponding~~ functionality of the component in the application.

15. (Currently amended) ~~A~~ The computer-readable medium ~~as recited in~~ of claim 11, wherein the computer-executable instructions for analyzing ~~one or more of the potential threats in terms of the model components~~ further comprise instructions for:

~~selecting a particular component of the model components; and~~

responsive to selection of a ~~selecting the~~ particular component in the logical model, displaying each other component ~~of the~~ in the logical model ~~components~~ that comprise at least a subset of similar potential security threats as the particular component.

16. (Currently amended) ~~A~~ The computer-readable medium ~~as recited in~~ of claim 11, wherein the computer-executable instructions for analyzing ~~one or more of the potential threats in terms of the model components~~ further comprise instructions for:

~~selecting a particular component of the model components; and~~

responsive to selection of a ~~selecting the~~ particular component in the logical model, automatically displaying each other component in ~~of~~ the logical model

~~components~~ that comprises a particular security threat similar to a security threat already addressed with respect to the particular component.

17. (Currently amended) ~~A~~ The computer-readable medium ~~as recited in~~ of claim 11, wherein the computer-executable instructions for analyzing ~~one or more of the potential security threats in terms of the model components in the logical model~~ further comprise instructions for~~:~~ ~~selecting~~ providing for selection of a particular threat associated with the security threat categories ~~of the potential threats~~ to indicate that the particular threat requires a threat mitigating implementation in a particular ~~mode~~ component of the logical model ~~components, the particular threat corresponding to the particular model component~~.

18. (Currently amended) ~~A~~ The computer-readable medium ~~as recited in~~ of claim 17, wherein the computer-executable instructions for ~~selecting~~ providing for selection of the particular threat further comprise instructions for identifying a priority that corresponds to the threat mitigating implementation.

19. (Currently amended) ~~A~~ The computer-readable medium ~~as recited in~~ of claim 17, wherein the computer-executable instructions for ~~selecting~~ providing for selection of the particular threat further comprise instructions for identifying a desired level of strength of technology with which to mitigate the particular threat.

20. (Currently amended) ~~A~~ The computer-readable medium ~~as recited in~~ of claim 17, wherein the computer-executable instructions for ~~selecting~~ providing for selection of the particular threat further comprise instructions for presenting

information associated with ~~selecting~~ a particular technology with which to mitigate the one or more potential threats in a physical implementation of the application.

21. (Original) A device comprising:

a memory comprising computer-executable instructions for providing application security threat-modeling;

a processor that is operatively coupled to the memory, the processor being configured to fetch and execute the computer-executable instructions from the memory, the computer-executable instructions comprising instructions for:

~~defining~~ providing class definitions defining attributes ~~a plurality~~ of model components representing ~~to represent~~ respective elements of an application, at least one attribute of the attributes associated with a ~~each~~ model component specifying a set of security threat categories potentially applicable to the model component ~~comprising a respective set of potential security threats~~;

presenting symbols associated with at least a subset of the model components on a display;

interconnecting respective ones of the at least a subset~~the model components~~ to form a logical model of the application; and

analyzing the logical model in view of security threat categories associated with respective ones of the model components in the logical model to identify a set of potential security threats to the application~~one or more of the potential security threats in terms of the model components in the logical model~~.

22. (Currently amended) ~~A~~ The device ~~as recited in~~ of claim 21, wherein the model components comprise a module, a port, a store, or a wire.

23. (Currently amended) ~~A~~ The device ~~as recited in~~ of claim 21, wherein the security threat categories ~~potential security threats~~ comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation

24. (Currently amended) ~~A~~ The device ~~as recited in~~ of claim 21, wherein the computer-executable instructions for ~~defining the model components~~ providing further comprise instructions for determining the ~~respective~~ security threat ~~characteristics~~ categories for a component of the model components based on ~~the components corresponding~~ functionality of the component in the application.

25. (Currently amended) ~~A~~ The device ~~as recited in~~ of claim 21, wherein the computer-executable instructions for analyzing ~~one or more of the potential threats in terms of the model components~~ further comprise instructions for: ~~selecting a particular component of the model components; and~~ responsive to selection of a ~~selecting the~~ particular component of the logical model, displaying each other component of the logical model ~~model components~~ that comprise at least a subset of similar potential security threats as the particular component.

26. (Currently amended) ~~A~~ The device ~~as recited in~~ of claim 21, wherein the computer-executable instructions for analyzing ~~one or more of the potential threats in terms of the model components~~ further comprise instructions ~~for:~~

~~selecting a particular component of the model components; and~~ responsive to selection of a ~~selecting the~~ particular component of the model components, for automatically displaying each other component of the logical model ~~model components~~ that comprises a particular security threat similar to a security threat already addressed with respect to the particular component.

27. (Currently amended) ~~A~~ The device ~~as recited in~~ of claim 21, wherein the instructions for analyzing ~~one or more of the potential security threats in terms of the model components in the logical model~~ further comprise instructions for: ~~selecting~~ providing for selection of a particular threat associated with the security threat categories ~~of the potential threats~~ to indicate that the particular threat requires a threat mitigating implementation in a particular ~~mode~~ model component of the logical model ~~components~~, the particular threat corresponding to the particular model component.

28. (Currently amended) ~~A~~ The device ~~as recited in~~ of claim 27, wherein the computer-executable instructions for ~~selecting~~ providing for selection of the particular threat further comprise instructions for identifying a priority that corresponds to the threat mitigating implementation.

29. (Currently amended) ~~A~~ The device ~~as recited in~~ of claim 27, wherein the computer-executable instructions for ~~selecting~~ providing for selection of the particular threat further comprise instructions for identifying a desired level of strength of technology with which to mitigate the particular threat.

30. (Currently amended) ~~A~~ The device ~~as recited in~~ of claim 27, wherein the computer-executable instructions for ~~selecting~~ providing for selection of the particular threat further comprise instructions for presenting information associated with ~~selecting~~ a particular technology with which to mitigate the one or more potential threats in a physical implementation of the application.

31. (Currently amended) A computing device comprising:

processing means for presenting a user interface for application security threat-modeling, the ~~user interface~~ processing means comprising:

means for displaying and interconnecting a plurality of model components to design a logical model of an application, at least a subset of the model components comprising a corresponding set of potential security threat characteristics defined in a schema of class definitions for the model components;

means for specifying a component of the model components in the logical model; ~~and~~

means for identifying a set of potential security threats in view of one or more of module, port, store, or wire attributes associated with the at least a subset of model components that comprise the logical model; and

means for ~~addressing one or more of~~ selecting a particular solution to mitigate the potential security threats in ~~terms of the model components~~ in the logical model.

32. (Canceled)

33. (Currently amended) ~~A user interface as recited in~~ The computing device of claim 31, wherein the corresponding security threat characteristics comprise at least one subset of authentication, authorization, auditing, privacy, integrity, availability, and non-repudiation.

34. (Currently amended) ~~A user interface as recited in~~ The computing device of claim 31, wherein the processing means further comprise ~~further comprising:~~ means for selecting a priority that corresponds to the ~~one or more~~ potential security threats.

35. (Currently amended) ~~A user interface as recited in~~ The computing device of claim 31, wherein the means for selecting further comprise ~~further comprising:~~ means for specifying a desired level of strength of technology with which to mitigate the ~~one or more~~ potential security threats.

36. (Currently amended) ~~A user interface as recited in~~ The computing device of claim 31, wherein the processing means further comprise ~~further comprising~~ means for selecting a particular technology with which to mitigate the ~~one or more~~ potential security threats in a physical implementation of the application.